IN THE SPECIFICATION with reference to the translation of the application as amended during international preliminary examination, filed herewith:

Page 1, immediately following the title, please insert the following:

This is the U.S. national phase of International Application No. PCT/DE03/00760 filed March 10, 2003, the entire disclosure of which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The heading beginning on page 1, line 3 has been changed as follows:

~~Description:~~

The paragraph beginning on page 2, line 26 has been changed as follows:

The generation of a forgery-proof document in whose genuineness third parties have an interest, which is done by means of a cryptographic module containing asymmetrical keys and an algorithm to form check values, is generally carried out in the following manner: first of all, using the algorithm to form check values, a check value is formed that relates to the document that is to be secured. Then a private key in the cryptographic module is used to encrypt the check value. The combination of these two processes is referred to as the generation of a "digital signature["]."

The paragraph beginning on page 3, line 21 has been changed as follows:

With this known method, the problem exists that, in order to check the genuineness of a document, it is necessary to have information that is directly related to the document producer's use of keys by means of the cryptographic module. In the typical example described above for generating digital signatures, this is the public key of the document producer or of his cryptographic module, which has to be used for the checking procedure. In

the case of the signature of the public key by a certification agency, the entire set comprising the public key, the identification of the user of this key and the digital signature of the certification agency is designated as the "key certificate["]."

The paragraph beginning on page 4, line 22 has been changed as follows:

In order to overcome these known disadvantages, with a method of this generic type, it is disclosed in ~~this applicant's~~ German patent specification DE 100 20 563 C2 to generate a secret in a security module, to transfer the secret together with information that reveals the identity of the security module in encrypted form to a certification agency, to decrypt the secret in the certification agency, thus recognizing the identity of the security module, to subsequently encrypt the secret together with information on the identity of the document producer in such a way that only a checking station can carry out a decryption, in order to then transmit the secret to a document producer. With this method, the document producer enters his own data into the security module, whereby the data entered by the document producer himself is irreversibly linked to the secret by means of the security module and whereby the secret cannot be reconstructed.

The paragraphs beginning on page 5, line 16 have been changed as follows:

A method for providing mailpieces with postage indicia is known from ~~this applicant's~~ German Preliminary Published Application DE 100 20 402 A1. With this method, information that serves to generate a postage indicium is transmitted in encrypted form from a loading station to a crypto-module of a customer system and then serves to generate digital postage indicia. The postage indicium contains a hash value that is formed from the mailing data and from the information that was transmitted and stored temporarily in the crypto-module and also contains a "Crypto-String" encrypted in this information that can only be

decrypted in a mail center during the checking of the postage indicium, after which it is provided with a digital signature.

~~The applicant's~~ German Preliminary Published Application DE 100 20 566 A1 describes a method of the same type in which customers can load value amounts from a value transfer center and said value amounts can be consumed in order to print out digital postage indicia. Here, in particular, a customer system transmits a random number to the value transfer center and the latter encrypts the random number with a symmetrical key and sends it back to the customer system.

The postage indicia ~~is~~ are generated in the same manner as described in German Preliminary Published Application DE 100 20 402, whereby in particular, the encrypted random number can only be decrypted in a mail center.

On page 6, line 9 please insert a heading as follows:

GENERAL DESCRIPTION

The paragraphs beginning on page 6, line 10 have been changed as follows:

According to the invention, this objective is achieved by a method ~~according to Claim 1~~ for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator, including the steps of

generating random key information and forming encrypted checking information from the key information and from a transaction indicator in a cryptographically reliable contact station, encrypting the key information in the cryptographically reliable contact station, transmitting the encrypted checking information and the encrypted key information by the cryptographically reliable contact station to an intermediate station, the intermediate station

temporarily storing the encrypted key information and the encrypted checking information and subsequently transmitting this to a cryptographic module of a document producer at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station.

According to the invention, this objective is likewise achieved by a value transfer center ~~according to Claim 1~~ with an interface for loading monetary values, including an interface to receive encrypted information of a cryptographically reliable contact station and to temporarily store the received encrypted information as well as means for receiving value transfer requests by at least one cryptographic module and of forwarding the received encrypted information to the cryptographic module at a different point in time.

~~An advantageous refinement of the method and of the value transfer center are the subject matter of the subordinate claims.~~

The paragraph beginning on page 7, line 7 has been changed as follows:

The ~~invention comprises~~ disclosed method and value transfer center have numerous advantages. ~~It makes~~ They make it possible to generate forgery-proof documents in a large number of application cases, especially in those cases where no direct connection exists between the document producer and the reliable contact station. For example, in this manner, forgery-proof documents can be generated without the use of computers and/or a data connection to the reliable contact station.

The paragraph beginning on page 8, line 7 has been changed as follows:

An especially preferred embodiment of the invention is characterized in that the data entered by the document producer ~~is~~ are irreversibly linked to the key information by means of the cryptographic module.

On page 10, line 31 please add a heading as follows:

BRIEF DESCRIPTION OF THE DRAWINGS

The paragraph beginning on page 10, line 32 has been changed as follows:

Additional advantages, special features and practical refinements of the invention ensue from the ~~subordinate~~ appended claims and from the ~~presentation~~ description below of preferred embodiments making reference to the drawings.

On page 11, line 11 please insert a heading as follows:

DETAILED DESCRIPTION

The paragraphs beginning on page 12, line 17 have been changed as follows:

The described method is used in a modified form by the Deutsche Post for the production of Internet postage stamps under the designation "PC franking["]." In summary, it is characterized in that the genuineness of the documents can be checked without the use of key information that is inherent to the cryptographic module. Instead, the checking station relies in part on information from a reliable contact station.

The paragraph beginning on page 13, line 5 has been changed as follows:

1. Prior to the loading procedure between the specification center of the operator and the digital franking machine of the customer, the postal service provider electronically supplies the operator with machine-related information to be supplied to the digital franking machines in the future. This information ~~comprises~~ includes, among other things, key information for use in the machine as well as a so-called "ValidityString" that is used for the

later checking in the mail center as well as information on the credit status of the customer. Parts of this information are encrypted in such a way that they can only be decrypted within the franking machine.

The paragraphs beginning on page 16, line 24 have been changed as follows:

7. The seventh step relates to the communication between the non-reliable station and the cryptographic module, said communication preferably being secured by additional suitable means. After all, in actual practice, this is the communication between a specification center of a manufacturer and its franking machine with cryptographic module, information which has to be protected against manipulation precisely because of the loading amount that is being electronically exchanged. If this communication were not protected, then an unauthorized increase of the loading amount would be possible. Therefore, only in the sense of this invention is the specification center of the manufacturer considered to be a "non-reliable station["],"_ but in actual practice, it can certainly be classified as being reliable.

8. In ~~the eight~~ an eighth step, the key information that was encrypted in Step 3 is decrypted and subsequently stored. This key information is used later to secure documents by generating a check value. In order to prevent the above-mentioned plain text attacks, it is important that the key information cannot be read out of the cryptographic module but rather that it can only be used within the module by the processes that are likewise present in the cryptographic module.

The paragraphs beginning on page 18, line 2 have been changed as follows:

13. In ~~the~~ a thirteenth step, the document reaches the checking station where it is checked for its structural completeness and integrity. In the concrete application of the invention for checking postage indicia, additional congruence checks have to be carried out at this

station. Since in this case, the secured document matches the machine-readable postage indicium, this can be checked against other mailpiece information such as the address and the postage class as well as against general information such as the date. In this manner, it can be ruled out that an actually valid postage indicium is used to frank a mailpiece that does not go with this postage indicium.

14. In ~~the~~ a fourteenth step, the checking information encrypted in Step 2 is re-encrypted. The checking information comprising several components is broken down into its constituents once again. In addition to other information, in particular, the key information and the transaction indicator are obtained. The latter can serve for an additional checking procedure. Thus, for example, the identity of the customer or document producer, which has been deposited in the transaction indicator, can be compared to a positive list of acceptable document producers or to a negative list of unacceptable document producers deposited in the checking station.

15. In ~~the~~ a fifteenth step, analogously to Step 11, a check value is generated. According to the same method as in Step 11, the plain text information of the document present in the checking station uses the just-decrypted key information from Step 14 to form a check value. If different methods are possible for generating check values in the cryptographic module, then the concrete choice of the method likewise has to be attached to the document or transferred to the checking station in the document of the document producer.